**4 Reasons Why Your Company Should Get ISO 27001 Compliant**

With rising dependency on internet and advancement in technology, securing sensitive information has now become a matter of priority for every organization. Not only is it important to ensure smooth operations, it is also a matter of reputation in the eyes of potential customers. Increased awareness of information security management has lead most organizations to implement controls in one form or another. However, their effectiveness relies deeply on their monitoring and control. Organizations with a short-sighted approach only introduce security controls that deal with specific IT areas only and do not pay much heed to other non-IT assets. This results in many nonconformities and overall poses various threats to information security of organizational assets. To overcome these issues, ISO 27001 standard was introduced. Achieving and maintaining ISO 27001 certification gives your clients an assurance that your organization has implemented best-practice information security methods.

While there are numerous benefits of ISO 27001 accreditation, here we explain in detail 4 reasons why your company must comply with the standard.

1. **Gaining Competitive Edge**

In a market full of competitors, it is hard to differentiate yourself in the eyes of a customer. Being ISO 27001 certified gives you that competitive edge from your rival companies and can become your unique selling proposition. It gives your organization the ability to stand apart from your competitors especially for customers that deal with sensitive information.

As a market differentiator, with ISO 27001 certification, your company can gain competitive edge in the following ways:

* Because your potential customers will certainly be apprehensive about their data security, having ISO 27001 certification will ensure your customers that you have a proactive approach towards information security threats and your organization is adopting best-practices to minimize threats.
* When signing a contract, being an ISO 27001 certified organization, you will appear more credible and reliable as compared to one that is not. Winning or losing a tender can rely heavily upon conformity and nonconformity to the standard respectively.
* It will also help you compete with foreign competitors and allow you to develop further into global market. In most countries, ISO 27001 compliance is one of the major requirements of supply chain.
* Being ISO 27001 compliant removes the hassle of completing in-depth security questionnaires and responding to auditors for every new client.
* With a good working relationship with existing clients, it also proves your organization’s adherence to best practices and helps retain longstanding customers.

1. **Avoiding Financial Loss Resulting from Security Breach**

As an organization seeking ISO 27001 compliance, you will definitely be concerned about the costs associated with the certification. It may be hard to decide how the costs of gaining and maintaining ISO 27001 compliance would relate to those incurred otherwise i.e. in case of breach of data, service interruptions, or perhaps a disgruntled employee. Although there is no technology or methodology to determine the amount of expenses reduced as a result of ISO 27001 compliance, you must still consider that it is better to comply with the standard rather than not, because of the following reasons:

* Implementing information security may seem like a cost with no financial gain at first, but it is definitely a gain when incidents occur less frequently and as a result, expenses to resolve those incidents are reduced.
* Breach of data not only results in leakage of organizational secrets, it also turns out exceptionally expensive. According to the “2015 Cost of Data Breach Study: Global Analysis” by IBM and Ponemon Institute, the average total cost of data breach was estimated to be $3.79 million, which amounts to 23% increase in the past two years.
* As ISO 27001 is a globally accepted standard for Information Security of information assets, compliance to the standard can help organizations avoid heavy fines and penalties that may result otherwise.

1. **Ensuring Data Privacy and Integrity**

Maintaining data privacy and integrity is yet another important concern for organizations both in terms of customers and employees. Especially, organizations that hold valuable personal data of clients need to ensure that it is kept secure and in safe hands. An Information Security Management System (ISMS) is a steadfast way to ensure effective management of information security and reduction of potential risks associated with breach of data. Hence, you need to consider the implementation and management of your organization’s ISMS based on internationally acclaimed information security standard ISO 27001 because of the following reasons:

* When it comes to securely storing the data, implementing access control, using it safely and only on purpose, and securely destroying it when no longer needed, the most reliable way is to do so according to ISO 27001.
* ISO 27001, through its systematic approach, helps in identifying, managing and reducing the severity of regular threats to your information.
* Being an ISO 27001 company ensures the protection of your information assets and hence reduces the probability of being faced with legal persecution and losing clients trust because of data breaches.
* ISO 27001 procedures enable you to promptly detect an incident of security breach and take planned action.
* It ensures data integrity with the help of its access control, data backup and data organization procedures. This allows the separation of affected data from the rest and rectifying it in case of a security breach.

1. **Defining Information Handling Roles and Responsibilities**

Though this may be the most underestimated reason to achieve ISO 27001 compliance, it is equally as important as the other ones in the long run. For an organization that experiences sudden growth, it is only a matter of time before it faces problems relating to roles and responsibilities of information assets. Going for ISO 27001 compliance automatically makes you precisely define roles and responsibilities and strengthen your organizational structure. Moreover, it ensures the following:

* It administers you to define who will make the decisions, who will hold the responsibility of information assets and who will be in charge of authorizing access to information.
* It covers the entire organization as a whole, including staff, technology, procedures, etc. and hence, helps develop an information security conscious organizational culture.
* It makes information security a priority for senior management and requires the management to state ISMS roles and responsibilities.
* It requires organizations to conduct regular information security awareness and training programmes, which in turn reduces employee-related security breaches.

As a conclusion, ISO 27001 brings in much more benefits to organizations than the ones described above. It is not a mere certification to show to the world but a real proof of how your organization takes the matter of information security seriously and professionally.

It allows organizations to provide informed decisions based upon risk management and continuous improvement cycle. This helps managers proactively determine overall cost benefit analysis/ROI by deciding how many people need to be hired, what tools should be acquired, which systems should be audited, how incidents should be responded, etc.

As most clients require ISO 27001 as a prerequisite or at least with security controls same as those of ISO 27001, organizations with ISO 27001 certification are able to exhibit fast turnaround time when submitting tenders to their potential clients.

Implementation of the latest version of the standard, ISO 27001: 2013 ensures C level corporate governance through an automatic integration of all other standards such as Business Continuity Management ISO 22301, IT Service Management (ISO 20000-1), Quality Management (ISO 9001), Environmental Management (ISO 14001), etc. Because of the similarity in their structures, managers can adapt a system of integrated procedures based upon the standards, thus saving time and financial costs.

20

Aligning ISO/IEC 27001 to the new structure will help organizations wanting to implement more than one management system at a time. The similarity in structure between the standards will save organizations money and time as they can adopt integrated policies and procedures.

For example, an organization might want to integrate their information security system (ISO/IEC 27001) with other management systems such as the business continuity management (ISO/IEC 22301), IT service management (ISO/IEC 20000-1) or quality management (ISO 9001).